Administration W2K: Audit

Audit

- enregistrer les activités des utilisateurs et du système d'exploitation
- sous forme d'entrées dans le journal « Sécurité »
- 3 motivations courantes:
  - sécurité, surveillance de l'utilisation des ressources
  - débogage
- 2 étapes pour la mise en place
  - configurer la stratégie d'audit
  - activer l'audit sur les objets à auditer

Stratégie d'audit

- type de stratégie de sécurité qui précise quelles activités doivent être auditées.
- 9 types de stratégies d'audit:
  - événement de connexion (ouverture/fermeture d'une session locale ou via réseau)
  - événement de connexion aux comptes: authentification d'un utilisateur
  - gestion des comptes
  - modification de stratégie
  - utilisation de privilèges
  - suivi des processus : une application effectue une

Stratégie d'audit

- 9 types de stratégie d'audit (suite):
  - accès au service d'annuaire (accès à un objet AD)
  - accès aux objets (fichiers, dossiers, ...)
- Ces deux derniers paramètres obligent à préciser :
  - quels objets (fichiers, imprimantes, objets AD) auditer
  - quels opérations auditer (lecture, écriture, création)
- 4 valeurs possibles pour les paramètres :
  - pas d'audit, réussite uniquement, échec uniquement
  - réussite et échec

Stratégie d'audit: valeurs par défaut:

paramètre de stratégie d'audit	Valeur par défaut
événements de conn. aux comptes	Réussite
gestion des comptes	Réussite (Contr. Dom.), pas d'audit sinon
accès aux serv. d'annuaire	Pas d'audit
événements de connexion	Réussite
Accès aux objets	Pas d'audit
Modification de stratégie	Pas d'audit
Utilisation de privilèges	Pas d'audit
Suivi des processus	Pas d'audit

Options de sécurité

- auditer l'accès des objets système globaux:
  - active l'audit mutex, sémaphores, ...
- auditer l'utilisation des provilèges de sauvegarde et de restauration:
  - génére un événement d'audit pour chaque sauvegarde/restauration (suppose que « auditer l'utilisation des privilèges » soit activé)
- arrêter immédiatement le système s'il n'est pas possible de se connecter aux audit de sécurité:
  - arrêt si le journal de sécurité est plein. L'administrateur pourra ouvrir une session pour corriger le problème

Configurer un stratégie d'audit

- stratégie locale dans un groupe de travail:
  - Outil d'administration/Stratégie de sécurité locale/paramètres de sécurité/stratégie locale/stratégie d'audit/...
- stratégie locale dans un domaine:
  - idem ou, sur un contrôleur de domaine: stratégie de sécurité du contrôleur de domaine
- stratégie d'audit dans un domaine
  - via un GPO: configuration ordinateur/paramètres windows/paramètres de sécurité/stratégies locales/stratégies d'audit

Configurer les options de sécurité pour l'audit

auditer les objets d'AD

- configurer la stratégie d'audit pour auditer les « accès au service d'annuaire »
- activer l'affichage des fonctionnalités avancées: utilisateurs et ordinateur AD/Affichage/fonctionnalités avancées
- clic droit sur un conteneur/propriétés/sécurité/paramètres avancés/audit/ajouter un utilisateur ou un groupe/OK/sélectionner les types d'évènements à auditer

auditer les événements du système de fichiers

- configurer la stratégie d'audit pour auditer les « accès aux objets »
- dans l'onglet sécurité des dossiers/fichiers: paramètres avancés/audit/ajouter un utilisateur ou un groupe/OK/sélectionner le type d'évènements à auditer

Audit: remarques

- trop auditer nuit fortement aux performances
- auditer augmente le nombre d'événement stockés dans les journaux d'événement
  - penser à les configurer
  - penser à les sauvegarder (voir les centraliser sur un poste de travail dédié)
  - être attentif à leur taille et l'espace disque
- qui peut auditer
  - les administrateurs
  - les utilisateurs ayant le droit « gérer le journal d'audit et de sécurité » dans la stratégie de groupe.

Audit: demo

- mise en place
- demo et lecture du journal